In the claims:

1. (currently amended) A method of securing packet data transferred between a first and second member of a private network coupled to client edge devices over a backbone comprising a plurality of provider devices including provider edge devices, the backbone operating according to a routing protocol, the method comprising the steps of:

encapsulating a private address of a packet from the first member in a public address of the packet to generate a tunneled packet;

transforming, at a client edge device, the tunneled packet by first applying a group security association associated with the private network to the tunneled packet to provide a secure tunneled packet and then updating a field in the secure tunneled packet in accordance with the routing protocol of the backbone to provide a client transformed packet;

forwarding the client transformed packet to a provider edge device; and

replacing, at the provider edge device, the a destination field of the packet with a group identifier associated with the private network for routing the packet across the backbone .

2. (cancelled)

3. (cancelled)

4. (cancelled)

5. (cancelled).

6. (original) The method according to claim 1, wherein the group security association is associated with each member of the private network.

7. (original) The method according to claim 1, further comprising the steps of:

each member of the private network registering with a global security server;

the global security server forwarding the group security association to each member of the private network.

8. (original) The method according to claim 7 including the step of the global security server periodically forwarding a new group security association to each member of the private network.

9. (currently amended) A method of securing packet data transferred between a first and second member of a private network over a backbone, the first and second member of the private network being coupled to respective client edge devices and the backbone comprising a plurality of provider devices including provider edge devices, the backbone operating according to a routing protocol, the method comprising the steps of:

determining, responsive to a gateway address of a packet, whether ~~routing information associated with~~ a packet received from a client edge device at a provider edge device of the backbone has been transformed to secure packet data transferred across ~~according to the routing protocol of~~ the backbone ~~background~~;

~~determining whether the packet is a member of the private network;~~ and

modifying at least one field of the packet to replace a destination address of the packet with a group identifier associated with ~~according to a routing protocol of~~ the private network responsive to a determination that the gateway address of the packet indicates that the packet is a member of the private network.

10. (cancelled)

11. (currently amended) ~~An apparatus at a node~~ A system for transforming packets for forwarding between a plurality of members coupled to client edge devices of a private network over a backbone comprised of a plurality of provider devices including provider edge devices in a scalable private network, wherein the backbone operates according to a protocol, the apparatus comprising:

a key table, the key table including a security association for each private network that the node is a member;

a client edge device including:

a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address including a gateway address and a destination address to provide a secured packet; and

transform logic operable to apply a security association to each packet transmitted by the client edge device to the backbone

a provider edge device coupled to the client edge device, the provider edge device comprising a virtual route forwarding table for storing group identifiers associated with destination addresses and~~, the transform logic including~~ means, responsive to the gateway address of the public address, for selectively ~~for~~ updating the destination field of the packet with a group identifier for routing the packet across ~~a field of the secure packet in accordance with a protocol of~~ the backbone.

12. (cancelled)

13. (currently amended) A provider edge node in a backbone of a scalable private network, for transforming packets forwarded between a plurality of members of the scalable private network over the backbone, wherein the backbone operates according to a protocol, the provider node comprising:

a routing table, operable to determine a next hop routing address for each packet received at the provider node, the routing table operating responsive to a field of the packet arranged according to the protocol of the backbone; and

means for updating a destination field of the packet to replace a destination identifier with a group identifier prior to the routing of the packet if it is determined that the source address of the packet corresponds to a gateway address indicating that the packet is forwarded between members of the scalable private network.

14. (currently amended) The provider node of claim 13, wherein the ~~means for updating replaces a destination field of the packet with~~ group identifier is a group identifier of the private network.

15. (currently amended) A system for providing secure packet transmission between members of a scalable private network over a backbone, the system comprising:

a first node, coupled to a backbone, the first node being a member of the private network and comprising:

a table for storing a group security association associated with the private network;

a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address to provide a secured packet;

transform logic operable to apply a security association to each packet transmitted to the backbone, the transform logic including means for updating a field of the secure packet in accordance with a protocol of the backbone; and

a provider node in the backbone operating according to a routing protocol, the provider node comprising:

a routing table, operable to determine a next hop routing address for each packet received at the provider node~~, the routing table operating responsive to a field of the packet arranged according to the protocol of the backbone~~; and

means for updating a destination address field of the packet to replace the destination address with a group identifier prior to the routing of the packet if it is determined that a source address of the packet indicates that the packet is forwarded between members of the scalable private network.